Théorie de Galois

I Corps des racines d'un polynôme. 1ère exposé : 1h30 § I à III inclus
II groupes de Galois.
III Extensions galoisiennes.
IV Théorèmes fondamentaux de la Théorie de Galois. (cf résumé)
V Application : Recherche des sous-corps d'une extension galoisienne de $\mathbb{Q}$
VI Application : Théorème de d'Alembert-Gauss.
VII Application : Equations résolubles par radicaux

Tous les corps intervenant ici sont commutatifs.

I Corps des racines d'un polynôme

(Toute cette partie I est recopiée et mise en forme dans mon exposé 5 en avril 2008)

1) Tout morphisme de corps est un monomorphisme (en effet : si $\varphi : K \to K^*$ est un morphisme de corps, $\varphi(x)=0$ et $x \neq 0$ alors il existe $x' \in K$ tq $xx'=1$ d'où $\varphi(x).\varphi(x') = 1$ ie $0=1$, faux)

2) Tout isomorphisme de corps $\varphi : K \to K^*$ peut être prolongé en un isomorphisme (encore noté φ) :

$$\varphi : K[X] \longrightarrow K^*[X]$$
$$P(X) = \sum_{i=0}^{n} a_i X^i \longmapsto P^*(X) = \sum_{i=0}^{n} \varphi(a_i) X^i$$

P^* est l'homologue de P par φ.

* $\forall \alpha \in K \quad \varphi(P(\alpha)) = (\varphi P)(\varphi(\alpha))$
donc φ applique les zéro de P sur les zéro de $\varphi(P) = P^*$

* P inéductible sur $K \iff P^*$ inéductible sur K^*

En effet, si $\deg P \neq 0$:
P réductible $\iff \exists Q, R \quad P = QR \quad Q \notin K$ et $R \notin K$
$\Rightarrow P^* = Q^* R^*$ avec $Q^* \notin K^*$ et $R^* \notin K^* \iff P^*$ réductible
La preuve est identique dans l'autre sens (φ étant un isomorphisme) :

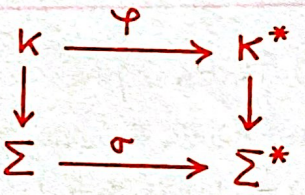
© MAI 92

3) Soit $f \in K[X]$. Un corps de factorisation de f sur K est une extension finie de K dans laquelle f admet toute ses racines (ie s'écrit comme produit de facteurs du 1er degré)
On montre l'existence d'un corps de factorisation de f en itérant le procédé d'adjonction symbolique d'une racine (Querré Th 2 p 93)

Un corps des racines de f sur K est un corps de factorisation minimal de f sur K, ie :
- un corps de factorisation L de f sur K
- si L' est un autre corps de factorisation de f tq $K \subset L' \subset L$, alors $L' = L$

Théorème : Soient

$\varphi : K \to K^*$ isomorphisme de corps
$f \in K[X]$
$f^* = \varphi(f)$ l'homologue de f dans $K^*[X]$
Σ (un / le) corps des racines de f
Σ^* un " " de f^*



1) Il existe un isomorphisme $\sigma : \Sigma \to \Sigma^*$ prolongeant φ
2) Si f est séparable (ie n'a que des racines distinctes dans son corps des racines Σ), il y a exactement $n = [\Sigma : K]$ isomorphismes $\sigma : \Sigma \to \Sigma^*$ prolongeant φ.

(Querré Th 1 p 99 et Th 2 p 100)

• Pb : pour définir un polynôme séparable, il faut d'abord avoir l'unicité du corps des racines.

preuve : Les 2 parties se montrent par récurrence sur $n = [\Sigma : K]$ et débutent ainsi :

Si $n = 1$, c'est trivial. Si $n > 1$, il existe une racine α de f n'appartenant pas à K. Soit $p = \mathrm{Irr}(\alpha, K, X)$ le polynôme irréductible de α.
$\deg p = d > 1$.

Soit $p^* = \varphi(p)$ l'homologue de p. p^* sera irréductible sur K^* et si $\sigma : \Sigma \to \Sigma^*$ prolonge φ, alors $\sigma(\alpha)$ sera une racine de p^*.

preuve de 1) :

Soit β une racine de p^*.

$$\Psi : \begin{array}{ccc} K(\alpha) & \longrightarrow & K^*(\beta) \\ \sum_{i=0}^{d-1} a_i \alpha^i & \longmapsto & \sum_{i=0}^{d-1} a_i^* \beta^i \end{array} \qquad \text{où } a_i^* = \varphi(a_i)$$

est un isomorphisme de corps prolongeant φ.

Comme $[\Sigma : K(\alpha)] = \frac{n}{d} < n$, l'hypothèse récurrente montre l'existence de σ prolongeant Ψ et rendant le diagramme suivant commutatif :

$$\begin{array}{ccc} K & \xrightarrow{\varphi} & K^* \\ \downarrow & & \downarrow \\ K(\alpha) & \xrightarrow{\Psi} & K^*(\beta) \\ \downarrow & & \downarrow \\ \Sigma & \xrightarrow{\sigma} & \Sigma^* \end{array} \qquad (*)$$

preuve de 2) : Si p est séparable, p^* le sera aussi (preuve : notons σ un prolongement de Σ dans Σ^*. On a vu qu'il existait au 1). p étant séparable : $p(X) = \prod_{i=1}^{d} (X - \alpha_i)$, les α_i étant tous distincts 2 à 2, donc $\sigma p(X) = \prod (X - \sigma(\alpha_i))$, $\sigma(\alpha_i)$ distincts 2 à 2, ie $\sigma p = p^*$ est séparable)

$\deg p^* = d$ donc p^* aura d racines distinctes.

Ψ devant nécessairement appliquer une racine de p sur une racine de p^*, on constate qu'il y a d choix possibles pour $\Psi(\alpha)$.

Le diagramme $(*)$ permet de conclure : on prolongera Ψ de $[\Sigma : K(\alpha)] = \frac{n}{d}$ façons possibles (hypothèse récurrente), soit au total $\frac{n}{d} \times d = n$ façons d'obtenir σ.

CQFD

Corollaire : Le corps des racines Σ d'un polynôme f sur K est unique à un K-isomorphisme près.

Le 1) du Th. préc. donne avec $\varphi = Id_K$:

$$\begin{array}{ccc} K & \xrightarrow{Id_K} & K \\ \downarrow & & \downarrow \\ \Sigma & \xrightarrow{\sigma} & \Sigma^* \end{array}$$

où σ est un K-isomorphisme.

CQFD [Recopié en cinq exemplaires jusqu'ici !]

II Groupes de Galois

Soit K une extension du corps k. Le groupe de Galois $G(K/k)$ de K sur k est le groupe des k-automorphismes de K

ex : $k = \mathbb{Q}$ $\quad K = \mathbb{Q}(i, \sqrt{2})$

Soit $F = \mathbb{Q}(i)$. $k \subset F \subset K$ et $G(K/k) \supset G(K/F)$ car tout F-automorphisme de K sera, à fortiori, un k-automorphisme.

$\mathrm{Irr}(i, \mathbb{Q}, X) = X^2 + 1$ $\quad$ donc $\quad [F : \mathbb{Q}] = 2$

$\mathrm{Irr}(\sqrt{2}, F, X) = X^2 - 2$ $\quad$ donc $\quad [K : F] = 2$

F est le corps des racines de X^2+1 donc $\mathrm{Id}_{\mathbb{Q}}$ se prolonge en un $\mathbb{Q}$-isomorphisme de F de 2 façons :

$$\sigma_1 = \mathrm{Id}_F \quad \text{ou} \quad \sigma_2 : F \longrightarrow F, \quad a+bi \longmapsto a-bi \qquad a, b \in \mathbb{Q}$$

K est aussi le corps des racines de $X^2 - 2$ sur F, donc σ_1 (resp. σ_2) se prolonge à K de 2 façons :

$$\tau_1 = \mathrm{Id}_K$$

$$\tau_2 : \alpha + \beta\sqrt{2} \longmapsto \alpha - \beta\sqrt{2} \qquad \alpha, \beta \in F$$

$$\tau_3 : \alpha + \beta\sqrt{2} \longmapsto \overline{\alpha} + \overline{\beta}\sqrt{2}$$

$$\tau_4 : \alpha + \beta\sqrt{2} \longmapsto \overline{\alpha} - \overline{\beta}\sqrt{2}$$

$G(K/k)$ est un groupe à 4 éléments, isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ puisque $\tau_i^2 = \mathrm{Id}_K$ pour tout i.

Enfin : $G(K/F) = \{\tau_1, \tau_2\}$

Soit $f \in k[X]$. Le groupe de Galois du polynôme f sur k est $G(K/k)$ où K est le corps des racines de f sur k.

Proposition : Soit $G(K/k)$ le groupe de Galois du polynôme $f \in k[X]$

1) $\#G(K/k)$ divise $r!$ où r est le nombre de racines de f dans K.
2) f séparable sur $k \Rightarrow \#G(K/k) = [K:k]$

preuve :

1) Soient $\alpha_1, \dots, \alpha_r$ les racines de f dans K.

Si $\sigma \in G(K/k)$, σ est un k-automorphisme de K et induit une permutation π_σ dans l'ensemble $\{\alpha_1, \dots, \alpha_r\}$ des racines.

(en effet : $\sigma(f(\alpha)) = (\sigma f)(\sigma(\alpha))$ donc $f(\alpha)=0 \Rightarrow (\sigma f)(\sigma(\alpha))=0$
$\Rightarrow f(\sigma(\alpha))=0$ car $\sigma|_k = Id_k$ entraîne $\sigma f = f$)

D'où le monomorphisme :

$$\begin{array}{ccc} G(K/k) & \longrightarrow & \mathcal{S}_r \\ \sigma & \longmapsto & \pi_\sigma \end{array}$$

et $\#G(K/k)$ divise $r!$

2) Si f est séparable, il existe exactement $[K:k]$ isomorphismes prolongeant Id_k d'après le Th. I.

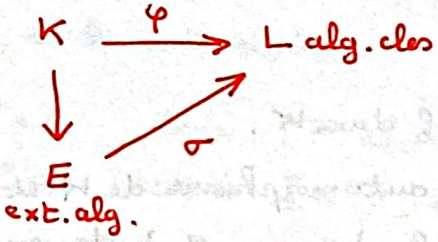
CQFD

III Extensions galoisiennes

a) On aura besoin du résultat suivant :

Théorème 1 : K corps
E ext. algébrique de K
L corps alg. clos
$\varphi : K \longrightarrow L$ monomorphisme

1) Il existe un monomorphisme $\sigma : E \longrightarrow L$ prolongeant φ :



2) Si E est alg. clos et si L est une ext. alg. de $\varphi(K)$, tout monomorphisme $\sigma : E \longrightarrow L$ prolongeant φ est un isomorphisme.

(Queré Th 2 p 97)

preuve :

1) Soit Σ l'ensemble des couples (F, ψ) où $\begin{cases} F = \text{sous-corps de } E \text{ contenant } K \\ \psi : F \longrightarrow L \text{ monomorphisme prolongeant } \varphi \end{cases}$

Σ est ordonné par la relation :

$$(F, \psi) \leqslant (F', \psi') \iff F \subset F' \text{ et } \psi'|_F = \psi$$

$\Sigma \neq \emptyset$ (car $(K, \varphi) \in \Sigma$) et Σ est inductif (en effet, si $\{(F_i, \psi_i)\}_{i \in I}$ est une famille totalement ordonnée de Σ, $F = \bigcup_{i \in I} F_i$ et $\psi : F \longrightarrow L$ définie par recollement des F_i montre l'existence d'une borne supérieure (F, ψ) de $\{(F_i, \psi_i)\}_{i \in I}$.)

L'axiome de Zorn affirme l'existence d'un élément (E', σ') maximal.

Montrons que $E' = E$: sinon il existerait $\alpha \in E \setminus E'$ et $\sigma' : E' \longrightarrow L$ pourrait être prolongé par un monomorphisme :

$$\sigma'' : E'(\alpha) \longrightarrow \sigma'(E')(\beta) \longrightarrow L$$

(en posant $\sigma''(\alpha) = \beta$ où β est une racine de $\sigma'(p) = p^* \in \sigma(E')[X]$ où p est le polynôme irréductible de α sur K, cf I.2)

$(E'(\alpha), \sigma'')$ appartiendrait à Σ ce qui contredit la maximalité de (E', σ').

2) $\varphi(K) \subset \sigma(E) \subset L$

E alg. clos $\Rightarrow$ $\sigma(E)$ alg. clos (Tout polynôme $P \in \sigma(E)[X]$ de degré ≥ 1 aura, en effet, au moins une racine dans $\sigma(E)$ car : $\exists P_1 \in E[X]$ $P = \sigma(P_1)$ donc il existe une racine α de P_1 dans E (E étant alg. clos). $\sigma(\alpha)$ sera bien une racine de $P = \sigma(P_1)$ dans $\sigma(E)$. CQFD)

Si L est algébrique sur $\varphi(K)$, L sera algébrique sur $\sigma(E)$ donc :

$$\forall \alpha \in L \quad \exists \beta \in \sigma(E)[X] \quad \beta(\alpha) = 0$$

Mais $\sigma(E)$ est algébriquement clos, donc $\alpha \in \sigma(E)$, puis $\sigma(E) = L$. σ sera surjective donc un isomorphisme.

CQFD

NB : Ce Théorème entraîne l'unicité de la clôture algébrique d'un corps K, une fois son existence démontrée.
(Queré Th 3 p 98 et Th 4 p 99)

Une extension galoisienne est une extension finie, normale et séparable

Cette définition nous impose de donner plus de détails :

b) Une extension finie est une extension obtenue par adjonction d'un nombre fini d'élément algébriques $\alpha_1, \dots, \alpha_n$ sur k, ie :

$$K = k(\alpha_1, \dots, \alpha_n)$$

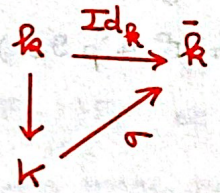
Il est équivalent de dire que K est un k-espace vectoriel de dimension finie (et on note $[K:k] = \dim_k K$ le degré, ou la dimension, de cette extension) (Querré p 91 ; Co2 p 93 et [A])

c) K est une extension normale de k si c'est une extension finie et si tout polynôme irréductible sur k possédant une racine dans K, possèdera toutes ses racines dans K.

Théorème 2 : Soit K une extension finie de k telle que $k \subset K \subset \bar{k}$ où $\bar{k}$ désigne la clôture algébrique de k.
~ entre :

1) K est une extension normale
2) K est le corps des racines d'un polynôme de $k[X]$
3) Tout monomorphisme $\sigma : K \longrightarrow \bar{k}$ prolongeant Id_k est un k-automorphisme de K

(Querré Th 1 p 103)



1) ⇒ 2) Soit $\alpha \in K \setminus k$ et $p = Irr(\alpha, k, X)$. p est irréductible sur k et possède la racine α dans K. K étant normal sur k, toutes les racines de p seront dans K et K contiendra le corps des racines Σ de p.
S'il existe $\beta \in K \setminus \Sigma$, on recommence avec $q = Irr(\beta, k, X)$. Le corps des racines Σ' de pq sera tel que $k \subsetneq \Sigma \subsetneq \Sigma' \subset K$, et ainsi de suite.
Le processus s'arrête car K est de degré fini sur k.

2) ⇒ 3) K est le corps des racines de $f \in k[X]$, soit :

$$K = k(\gamma_1, \dots, \gamma_r) \qquad \text{et} \qquad f(X) = a \prod_{i=0}^{n} (X - \gamma_i)$$

Tout monomorphisme $\sigma : K \to \bar{k}$ prolongeant Id_k transformera les racines de f en elles-mêmes car :

$$f(\gamma) = 0 \quad \Rightarrow \quad \sigma(f(\gamma)) = 0 \quad \Rightarrow \quad f(\sigma(\gamma)) = 0$$

donc sera à valeurs dans K.

On conclut grâce au :

lemme : K = ext. algébrique de k ; $\sigma : K \to K$ monomorphisme prolongeant Id_k $\Rightarrow$ σ est un k-automorphisme de K.

preuve : il faut montrer que σ est surjective.

$\forall \alpha \in K \quad \exists p = Irr(\alpha, k, X) \quad p(\alpha) = 0$

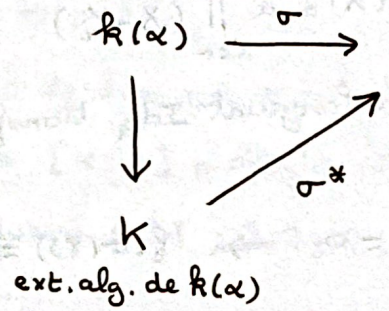
Soit K' le sous-corps de K engendré par k et les racines de p contenues dans K.
Si γ est une telle racine, $p(\gamma) = 0 \Rightarrow \sigma(p(\gamma)) = p(\sigma(\gamma)) = 0$.
σ applique donc les racines de p contenues dans K sur elles-mêmes.
$\sigma' \doteq \sigma|_{K'}$, sera donc un k-endomorphisme de K', injectif comme tous les morphismes de corps. K' étant un k-espace vectoriel de dimension finie, σ' sera bijective, ie un k-automorphisme de K' donc $\alpha \in \operatorname{Im}\sigma$. CQFD

3) ⇒ 1) Soit p un polynôme irréductible de $k[X]$ admettant une racine α dans K.
Notons $\sum$ le corps des racines de p et β une racine de p dans $\sum$.
On peut définir le monomorphisme :

$$\sigma : k(\alpha) \xrightarrow{\sim} k(\beta) \longrightarrow \sum \hookrightarrow \bar{k}$$
$$\sum_{i=1}^{n} a_i \alpha^i \longmapsto \sum_{i=1}^{n} a_i \beta^i \quad (\text{où } n = \deg p)$$

par $\begin{cases} \sigma|_k = Id_k \\ \sigma(\alpha) = \beta \end{cases}$

Comme K est une extension algébrique de $k(\alpha)$ et $\bar{k}$ est un corps alg. clos, σ se factorisera à travers K en un monomorphisme σ^* (Th. 1) :



Par hypothèse, σ^* sera un k-automorphisme de K, donc $\beta = \sigma(\alpha) \in K$. Toutes les racines de p seront bien dans K.

CQFD

Pro. 1 : $k \subset F \subset K$, K ext. (finie et) normale de k $\Rightarrow$ K = ext. normale de F

preuve : utiliser le 3) du Th. 2 (A Queré Co 2 p 104)

d) K est une extension séparable sur k si tout élément α de K est séparable sur k, ie est racine d'un polynôme séparable sur k. Un polynôme est séparable sur k s'il est dans k[X] et ne possède que des racines distinctes dans son corps des racines.

On aura besoin des 2 résultats :

Pro. 2 : $k \subset F \subset K$, K ext. séparable sur k $\Rightarrow$ { K séparable sur F ; F séparable sur k }

(Queré Th. 3 p 103). La preuve de cette proposition est facile.

Théorème 3 : Toute extension galoisienne est le corps des racines d'un polynôme séparable.
Si K est de caractéristique 0, la réciproque est vraie ; et on a même :
L = ext. galoisienne de K $\Leftrightarrow$ L = corps des racines d'un polynôme de K[X].
(A Queré p 104, Co 1 et Co 1 bis)

IV Théorèmes fondamentaux de la Théorie de Galois

Th.1 : Soient K un corps
G un sous-groupe du groupe $Aut(K)$ des automorphismes de K
$K^G \doteq \{x \in K \,/\, \forall \sigma \in G \;\; \sigma(x) = x\}$ = corps fixe de G

Alors K est une extension galoisienne de K^G, son groupe de Galois est $G(K/K^G) = G$ et $[K : K^G] = \#G$

preuve : Posons $k = K^G$ et $n = \#G$

a) K est une ext. séparable de k :

Soit $\alpha \in K$ et $A = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ un ensemble maximal d'éléments tels que $\sigma_1(\alpha), \dots, \sigma_n(\alpha)$ soient tous distincts.

$$\exists j \quad \sigma_j(\alpha) = \alpha \qquad (\text{car } Id_K(\alpha) = \alpha \text{ et } A \text{ maximal})$$

donc α est racine de $f(X) = \prod_{i=1}^{n} (X - \sigma_i(\alpha))$

$\forall \tau \in G$ $\tau\sigma_1(\alpha), \dots, \tau\sigma_n(\alpha)$ sont distincts, et comme A est maximal :

$$\{\tau\sigma_1(\alpha), \dots, \tau\sigma_n(\alpha)\} = \{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}$$

On en déduit :

$$\forall \tau \in G \qquad \tau f = f$$

Si $f(X) = \sum_{i=0}^{n} a_i X^i$, $\tau(a_i) = a_i$ donc $a_i \in K^G \doteq k$. Ainsi $f \in k[X]$ est un polynôme séparable qui s'annule en α : K sera séparable (donc algébrique) sur k.

Th.2 :: Alon

b) K est une ext. normale de k :

Le a) montre que :

$\forall \alpha \in K \quad \exists f \in k[X]$ tq $f(\alpha)=0$, et f se factorise en facteurs linéaires dans K.

Si p est un polynôme irréductible de $k[X]$ admettant une racine α dans K, on aura $p \mid f$ (p sera, en effet, le polynôme minimal de α, à une cte non nulle près) et p aura toutes ses racines dans K (car f a toutes ses racines dans K).

c) K est une ext. finie de k et $[K:k] \leq n$

Soit $\alpha \in K$. Le a) montre que α est racine d'un polynôme séparable de degré $\leq n$, de sorte que l'on puisse choisir un élément α de K de degré maximum m ($\leq n$).

Si $k(\alpha) \neq K$, il existe $\beta \in K \setminus k(\alpha)$ et K étant séparable sur k, le Th. de l'élément primitif (Th.2 p102) assure l'existence de $\gamma \in K$ tel que :

$$k(\alpha,\beta) = k(\gamma)$$

Mais $[k(\alpha,\beta):k] = \underbrace{[k(\alpha,\beta):k(\alpha)]}_{>1} \cdot \underbrace{[k(\alpha):k]}_{m} > m$, ce qui

contredit le caractère maximal de m.

Donc $K = k(\alpha)$ et $[K:k] = \deg \alpha = m \leq n$

d) Ainsi K est une extension galoisienne de k, donc sera le corps des racines d'un polynôme séparable g (Th III.3), et (Pro.II) :

$$\# G(K/k) = [K:k] = m$$

Mais $\underbrace{G}_{\text{cardinal } n} \subset \underbrace{G(K/k)}_{\text{cardinal } m} \Rightarrow n \leq m$

Finalement $n=m$ et $G(K/k) = G$.

CQFD

Th.2 : Soit K une extension galoisienne de k.

Alors :

1) $k = K^{G(K/k)}$ (= corps fixe de $G(K/k) \subset \mathrm{Aut}\, K$; sgroupe)

2) Si F est un corps intermédiaire (ie tq $k \subset F \subset K$), alors K est une ext. galoisienne de F.

3) Si $\mathcal{K}$ = famille des corps intermédiaires

$\mathcal{G}$ = " des sous-groupes de $G(K/k)$

l'application $\mathcal{K} \longrightarrow \mathcal{G}$ est bijective décroissante.

$F \longmapsto G(K/F)$

preuve : Posons $G = G(K/k)$

1) $k = K^G$?

On a $k \subset K^G$. Réc., soit $\alpha \in K^G$ et $\sigma : k(\alpha) \longrightarrow \bar{K}$ un monomorphisme prolongeant Id_k.

σ se prolonge en σ^* (Th III.1) :

$$\begin{array}{ccc} k(\alpha) & \xrightarrow{\sigma} & \bar{K} = \bar{k} \text{ alg.clos} \\ \downarrow & \nearrow_{\sigma^*} & \\ K & & \\ \text{ext.alg. de } k & & \end{array}$$

K étant une extension normale de k et $\sigma^* : K \longrightarrow \bar{K} = \bar{k}$ prolongeant Id_k, σ^* sera un k-automorphisme de K (Th III.2). On en déduit $\sigma^*(\alpha) = \sigma(\alpha) = \alpha$ (car $\alpha \in K^G$)

Il y a donc 1 seul automorphisme $\sigma : k(\alpha) \longrightarrow \bar{K}$ prolongeant Id_k.

α est séparable sur k. Si $p = \mathrm{Irr}(\alpha, k, X)$ est son polynôme irréductible, p est séparable sur k donc $\mathrm{Id}_k : k \longrightarrow k$ se prolongera en exactement $\deg p$ morphismes de $k(\alpha)$ dans $\bar{K}$ (associer à α l'une quelconque des $\deg p$ racines distinctes de p dans $\bar{K} = \bar{k}$)

Nécessairement $\deg p = 1$, donc $\alpha \in k$. On a bien prouvé que $K^G \subset k$.

2) $k \subset F \subset K$. D'après les Pro. III.1 et III.2 , K étant une ext. finie, normale et séparable de k , il en sera de même de K sur F .

3)
$$\begin{array}{ccc} K & \xrightarrow{\Psi} & G \\ F & \longmapsto & G(K/F) \end{array}$$

est bien définie car $G(K/F)$ est un sous-groupe de $G(K/k)$.

Si H est un sous-groupe de $G(K/k)$, $H \subset \mathrm{Aut}\, K$ et le Th.1 entraine :

$$G(K/K^H) = H \qquad \text{et} \qquad k \subset K^H \subset K$$

donc Ψ est surjective .

Si $G(K/F) = G(K/F')$, K est une extension galoisienne de F et de F' et le 1) ci-dessus permet d'écrire :

$$F = K^{G(K/F)} = K^{G(K/F')} = F'$$

donc Ψ est injective

La décroissance de Ψ est triviale (ie $F \subset F' \Rightarrow G(K/F) \supset G(K/F')$)

CQFD

Th.3 : K = ext. galoisienne de k

Si F et F' sont 2 corps intermédiaires isomorphes, alors les groupes de Galois $G(K/F)$ et $G(K/F')$ sont des sous-groupes conjugués de $G(K/k)$.

Il existe un k-isomorphisme λ prolongeant l'isomorphisme $F \to F'$:

$$\begin{array}{ccc} F & \xrightarrow{\sim} & F' \\ \downarrow & & \downarrow \\ K & \xrightarrow{\lambda} & K \end{array}$$

(en effet : K ext. galoisienne de $k \Rightarrow K$ = corps de racines d'un polynôme séparable de $k[X]$. K sera donc le corps des racines de ce même polynôme sur F, et sur F', et l'on peut appliquer le Th I)

$\sigma \in G(K/F) \Rightarrow \lambda\sigma\lambda^{-1} \in G(K/F')$ donc $\lambda\, G(K/F)\, \lambda^{-1} \subset G(K/F')$

$\sigma' \in G(K/F') \Rightarrow \lambda^{-1}\sigma\lambda \in G(K/F)$ donc $\lambda^{-1} G(K/F')\, \lambda \subset G(K/F)$

et l'on aura bien $\boxed{\lambda\, G(K/F)\, \lambda^{-1} = G(K/F')}$

CQFD

Th.4

K ext. galoisienne de k

F corps intermédiaire

1) F est normal sur $k \iff G(K/F) \triangleleft G(K/k)$

2) Si F est normal sur k, alors $G(K/k)/G(K/F) \simeq G(F/k)$

preuve : Posons $G = G(K/k)$

$H = G(K/F)$

a) Si F est normal sur k, on peut définir le morphisme de groupes

$$\begin{array}{rccc} h : & G(K/k) & \longrightarrow & G(F/k) \\ & \sigma & \longmapsto & \sigma|_F \end{array}$$

(En effet $\sigma|_F : F \longrightarrow K$ prolonge Id_k. On a le diagramme :

$$\begin{array}{ccc} k & \xrightarrow{Id_k} & K \subset \bar{k} \quad (\text{car } K \text{ ext. finie de } k \Rightarrow \bar{K} = \bar{k}) \\ \downarrow & \nearrow_{\sigma|_F} & \\ F & & \\ \text{normal sur } k & & \end{array}$$

F étant normal sur k, $\sigma|_F$ sera un k-automorphisme de F (Th III.2))

* h est surjective car tout k-automorphisme $\sigma' \in G(F/k)$ se prolonge en un monomorphisme $\sigma^* : K \longrightarrow \bar{K}$ suivant le diagramme (Th III.1)

$$\begin{array}{ccc} F & \xrightarrow{\sigma'} & \bar{K} \text{ alg. clos} \\ \downarrow & \nearrow_{\sigma^*} & \\ K & & \\ \text{ext. alg. de } F & & \end{array}$$

qui induit à son tour un k-automorphisme de K (car K est normal sur k et σ^* prolonge $Id_k : k \longrightarrow \bar{K}$ d'après le diagramme :

$$\begin{array}{ccccc} k & & \xrightarrow{Id_k} & & \\ \downarrow & & & & \\ F & \xrightarrow{\sigma'} & \bar{k} = \bar{K} = \text{clôt. alg. de } k \text{ et } K & \text{car } K = \text{ext. finie de } k. & \\ \downarrow & \nearrow_{\sigma^*} & & & \\ K & & & & \end{array}$$

on applique le Th III.2)

Clairement : $\sigma^*|_F = \sigma'$

* $\sigma \in \ker h \iff \sigma|_F = Id_F \iff \sigma \in G(K/F)$, donc $\ker h = G(K/F)$.

Donc $G(K/F) \lhd G(K/k)$ et par décomposition canonique de h :

$$\frac{G(K/k)}{G(K/F)} \simeq G(F/k)$$

b) Si F n'est pas normal sur k, il existe un monomorphisme $\lambda : F \to \overline{K}$ prolongeant Id_k et qui ne soit pas un k-automorphisme de F (Th III.2)

* On a $\lambda(F) \neq F$, sinon $\lambda : F \to F$, $\dim_k F < \infty$ et λ injective et k-linéaire entraineraient que λ est un k-automorphisme de F.

* $k \subset \lambda(F) \subset K$: en effet, si $\alpha \in F$ soit $p = Irr(\alpha, k, X)$.

$$p(\alpha) = 0 \Rightarrow \lambda(p(\alpha)) = 0 \Rightarrow p(\lambda(\alpha)) = 0 \quad (\lambda \text{ prolongeant } Id_k)$$

$\lambda(\alpha)$ sera donc une racine de p. K étant normal sur k, un polynôme irréductible p de $k[X]$ ayant une racine dans K aura toutes ses racines dans K. Ici, $\lambda(\alpha)$ appartiendra à K, donc $\lambda(F) \subset K$

* Ccl : $\lambda(F)$ et F sont 2 corps intermédiaires isomorphes mais distincts. Les groupes de Galois $G(K/\lambda(F))$ et $G(K/F)$ seront conjugués (Th.3) mais distincts (d'après la bijection du Th.2), donc $G(K/F)$ ne sera pas normal dans $G(K/k)$.

CQFD

V Application : recherche des sous-corps d'une extension galoisienne de $\mathbb{Q}$.

Le Th. IV.2 permet d'obtenir la liste des corps intermédiaires situés entre k et une extension galoisienne K de k à partir de la liste des sous-groupes du groupe de Galois de K sur k.

Rappelons que :

* Si K est une ext. de $\mathbb{Q}$, tout sous-corps de K sera un corps intermédiaire
* $\mathbb{Q}$ étant de caractéristique 0, K est une extension galoisienne de $\mathbb{Q}$ ssi c'est le corps des racines d'un polynôme f de $\mathbb{Q}[X]$ (Th III.3)

a) Cas de $f(X) = (X^2-2)(X^2-3)$ (queré ex48 p124)

$\Sigma = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ est le corps des racines de $(X^2-2)(X^2-3)$

$$\#G(\Sigma/\mathbb{Q}) = [\Sigma : \mathbb{Q}] = 4 \qquad \text{(Pro. II)}$$

puisque :

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ car $\mathrm{Irr}(\sqrt{2}, \mathbb{Q}, X) = X^2-2$

$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ car $\mathrm{Irr}(\sqrt{3}, \mathbb{Q}(\sqrt{2}), X) = X^2-3$

$\mathrm{Id}_{\mathbb{Q}}$ se prolonge de 2 manières en un $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\sqrt{2})$:

$$\tau_1 = \mathrm{Id}_{\mathbb{Q}(\sqrt{2})}$$

$$\tau_2 : \alpha = a + b\sqrt{2} \longmapsto \bar{\alpha} = a - b\sqrt{2} \qquad a, b \in \mathbb{Q}$$

τ_1 se prolonge en 2 $\mathbb{Q}$-automorphismes de Σ :

$$\begin{cases} \sigma_1 = \mathrm{Id}_{\Sigma} \\ \sigma_2 : \alpha + \beta\sqrt{3} \longmapsto \alpha - \beta\sqrt{3} \end{cases} \qquad \alpha, \beta \in \mathbb{Q}(\sqrt{2})$$

τ_2 se prolonge en :

$$\begin{cases} \sigma_3 : \alpha + \beta\sqrt{3} \longmapsto \bar{\alpha} + \bar{\beta}\sqrt{3} \\ \sigma_4 : \alpha + \beta\sqrt{3} \longmapsto \bar{\alpha} - \bar{\beta}\sqrt{3} \end{cases} \qquad \alpha, \beta \in \mathbb{Q}(\sqrt{2})$$

et $G(\Sigma/\mathbb{Q}) = \{ \underbrace{Id_\Sigma}_{\doteq i}, \sigma_2, \sigma_3, \sigma_4 \}$

Comme $\sigma_j^2 = Id_\Sigma$ pour tout j, $G(\Sigma/\mathbb{Q})$ est le groupe de Klein (ie isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). Les sous-groupes de $G \doteq G(\Sigma/\mathbb{Q})$ seront $\{i\}, \{i, \sigma_2\}, \{i, \sigma_3\}, \{i, \sigma_4\}, G$. Les corps intermédiaires F situés entre $\mathbb{Q}$ et $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ seront donc les corps fixes de ces groupes (Th IV.2), soit :

$$F_1 = \Sigma^{\{i\}} = \Sigma \qquad F_2 = \Sigma^{\{i,\sigma_2\}} = \mathbb{Q}(\sqrt{2}) \qquad F_3 = \Sigma^{\{i,\sigma_3\}} = \mathbb{Q}(\sqrt{3})$$

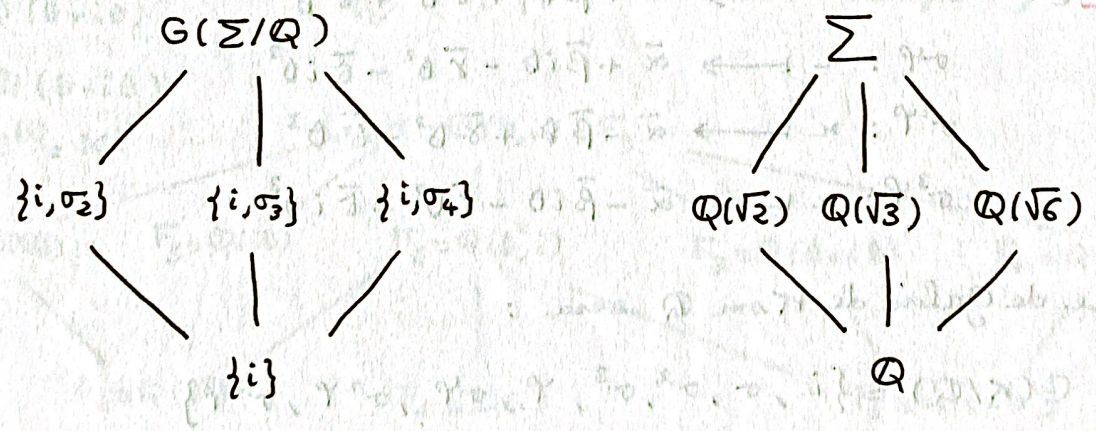
$$F_4 = \Sigma^{\{i,\sigma_4\}} \quad \text{et} \quad F_5 = \Sigma^{G} = \Sigma^{G(\Sigma/\mathbb{Q})} = \mathbb{Q} \qquad (\text{Th IV.2})$$

Explicitons F_4 : $F_4 = \{ \alpha + \beta\sqrt{3} \in \Sigma \ / \ \sigma_4(\alpha + \beta\sqrt{3}) = \alpha + \beta\sqrt{3} \}$

Comme $\left.\begin{array}{l} \bar{\alpha} - \bar{\beta}\sqrt{3} = \alpha + \beta\sqrt{3} \\ \alpha, \beta \in \mathbb{Q}(\sqrt{2}) \end{array}\right\} \Leftrightarrow \left\{\begin{array}{l} \alpha \in \mathbb{Q} \\ \beta = b\sqrt{2} \text{ où } b \in \mathbb{Q} \end{array}\right.$, on constate qu'un élément $\alpha + \beta\sqrt{3}$ sera dans F_4 ssi il s'écrit $a + b\sqrt{6}$ avec $a, b \in \mathbb{Q}$.

Donc $F_4 = \mathbb{Q}(\sqrt{6})$

Ccl : Liste des sous-groupes de $G(\Sigma/\mathbb{Q})$ et des sous-corps de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$:



Sous-groupes — Corps intermédiaires

ex : Mq $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ (Sol. : Soit $K = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, $(\sqrt{2}+\sqrt{3})^2 = 5 + 2\sqrt{6} \in K$ donc $\sqrt{6} \in K$. Par suite $\sqrt{6}(\sqrt{2}+\sqrt{3}) = 2\sqrt{3} + 3\sqrt{2} \in K$, donc $(2\sqrt{3}+3\sqrt{2}) - 2(\sqrt{2}+\sqrt{3}) = \sqrt{2} \in K$ puis $\sqrt{3} = (\sqrt{3}+\sqrt{2}) - \sqrt{2} \in K$. Finalement $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset K$. La réc. est évidente car toute comb. $\mathbb{Q}$-linéaire de $1, \sqrt{2}+\sqrt{3}, (\sqrt{2}+\sqrt{3})^2, \ldots$ sera comb. $\mathbb{Q}$-linéaire de $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$)

Voici la liste

b) Cas de $f(X) = X^4 - 3$ (traité en exemple dans Querré ex 4 p 122)

$f(X) = X^4 - 3$ est irréductible sur $\mathbb{Q}$ d'après le critère d'Eisenstein et ses racines sont $\{\pm\theta, \pm i\theta\}$ où $\theta = \sqrt[4]{3}$.

$K \doteq \mathbb{Q}(\theta, i)$ est le corps des racines de $f(X)$. C'est une extension de degré 8 car :

$$[K : \mathbb{Q}] = \underbrace{[K : \mathbb{Q}(i)]}_{4} \cdot \underbrace{[\mathbb{Q}(i) : \mathbb{Q}]}_{2} = 8$$

car $\mathrm{Irr}(\theta, \mathbb{Q}(i), X) = X^4 - 3$; car $\mathrm{Irr}(i, \mathbb{Q}, X) = X^2 + 1$

Il y a 2 monomorphismes de $\mathbb{Q}(i)$ prolongeant $\mathrm{Id}_{\mathbb{Q}}$:

$\Psi_1 = \mathrm{Id}_{\mathbb{Q}(i)}$

$\Psi_2 : \alpha = a + ib \longmapsto \bar{\alpha} = a - ib \qquad a, b \in \mathbb{Q}$

Chacun de ces monomorphismes se prolonge de 4 manières à K.

Notons $x = \alpha + \beta\theta + \gamma\theta^2 + \delta\theta^3$ un élément de K, où $\alpha, \beta, \gamma, \delta \in \mathbb{Q}(i)$.

Pour Ψ_1 : $i = \mathrm{Id}_K$

$\sigma : x \longmapsto \alpha + \beta i\theta - \gamma\theta^2 - \delta i\theta^3$ (quand $\theta \mapsto \theta$)

$\sigma^2 : x \longmapsto \alpha - \beta\theta + \gamma\theta^2 - \delta\theta^3$ (" $\theta \mapsto i\theta$)

$\sigma^3 : x \longmapsto \alpha - \beta i\theta - \gamma\theta^2 + \delta i\theta^3$ (" $\theta \mapsto -\theta$)

(" $\theta \mapsto -i\theta$)

Pour Ψ_2 :

$\varphi : x \longmapsto \bar{\alpha} + \bar{\beta}\theta + \bar{\gamma}\theta^2 + \bar{\delta}\theta^3$

$\sigma\varphi : x \longmapsto \bar{\alpha} + \bar{\beta} i\theta - \bar{\gamma}\theta^2 - \bar{\delta} i\theta^3$

$\sigma^2\varphi : x \longmapsto \bar{\alpha} - \bar{\beta}\theta + \bar{\gamma}\theta^2 - \bar{\delta}\theta^3$

$\sigma^3\varphi : x \longmapsto \bar{\alpha} - \bar{\beta} i\theta - \bar{\gamma}\theta^2 + \bar{\delta} i\theta^3$

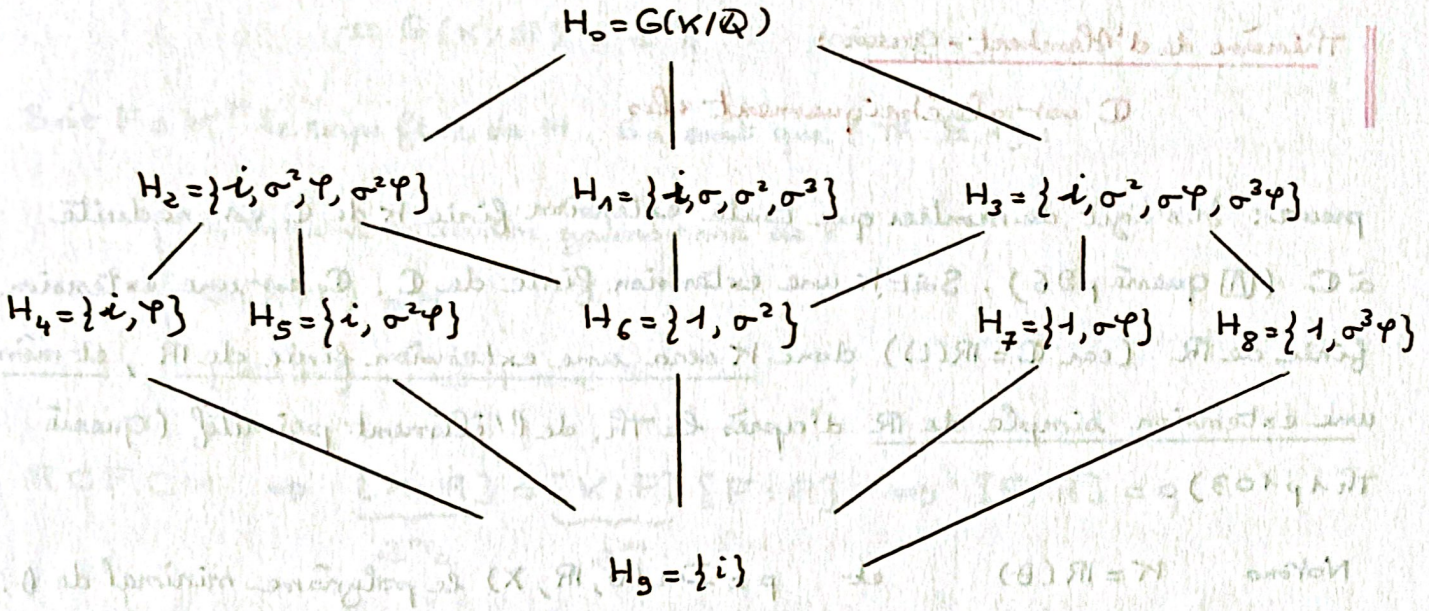
Le groupe de Galois de K sur $\mathbb{Q}$ sera :

$$G(K/\mathbb{Q}) = \{i, \sigma, \sigma^2, \sigma^3, \varphi, \sigma\varphi, \sigma^2\varphi, \sigma^3\varphi\}$$

On constate : $\begin{cases} \varphi\sigma = \sigma^3\varphi \\ \sigma^4 = i \\ \varphi^2 = i \end{cases}$

p 122)

Voici la liste des sous-groupes de $G(K/\mathbb{Q})$:



puis celle des sous-corps de K (détaillée dans [A] Queré p 123) :

$F_0 = K^{H_0} = \mathbb{Q}$

$F_1 = K^{H_1} = \{x \in K \,/\, \sigma(x) = x\} = \mathbb{Q}(i)$, et ainsi de suite ;

$F_2 = \mathbb{Q}(\theta^2)$

$F_3 = \mathbb{Q}(i\theta^2)$

$F_4 = \mathbb{Q}(\theta)$

$F_5 = \mathbb{Q}(i\theta)$

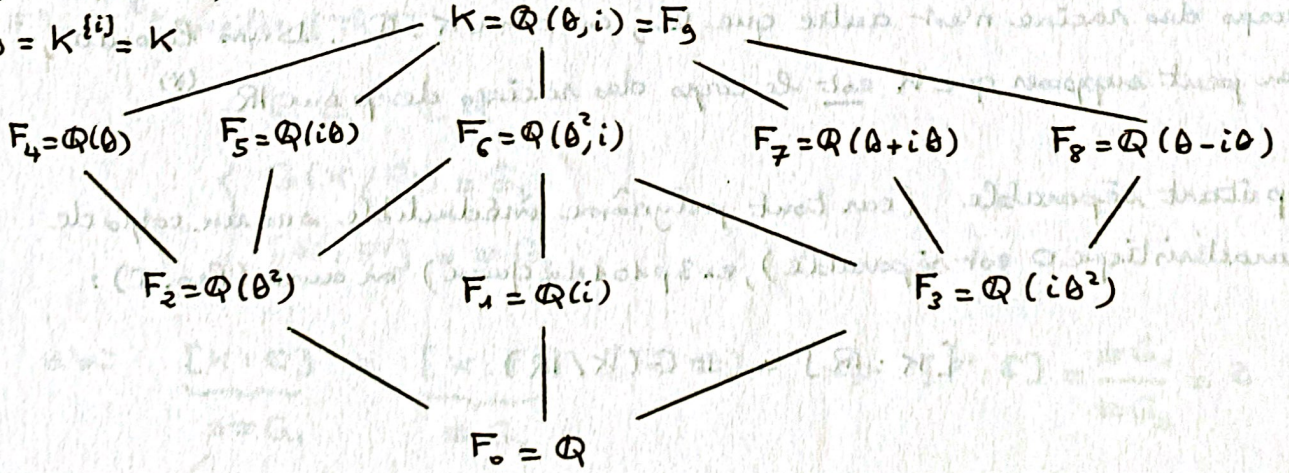
} ces 2 là sont isomorphes (car θ et $i\theta$ sont des racines du même polynôme irréductible $f = X^4 - 3 \in \mathbb{Q}[X]$, donc les corps $\mathbb{Q}(\theta)$ et $\mathbb{Q}(i\theta)$ obtenus par adjonction d'une racine de f seront isomorphes à $\mathbb{Q}[X]/(f)$ – cf Queré III.A.1 "extensions simples".)

$F_6 = \mathbb{Q}(\theta^2, i)$

$F_7 = \mathbb{Q}(\theta + i\theta)$

$F_8 = \mathbb{Q}(\theta - i\theta)$

$F_9 = K^{\{i\}} = K$



VI Application : Théorème de d'Alembert - Gauss

Théorème de d'Alembert - Gauss :

$\mathbb{C}$ est algébriquement clos

preuve : Il s'agit de montrer que toute extension finie K de $\mathbb{C}$ est réduite à $\mathbb{C}$ (A queré p96). Soit K une extension finie de $\mathbb{C}$. $\mathbb{C}$ est une extension finie de $\mathbb{R}$ (car $\mathbb{C} = \mathbb{R}(i)$) donc K sera une extension finie de $\mathbb{R}$, et même une extension simple de $\mathbb{R}$ d'après le Th. de l'élément primitif (queré Th 1 p103).

Notons $K = \mathbb{R}(\theta)$ et $p = Irr(\theta, \mathbb{R}, X)$ le polynôme minimal de θ.

On aura $[K : \mathbb{R}] = \deg p$, et comme un polynôme irréductible de $\mathbb{R}[X]$ est de degré 1 ou pair (car tout polynôme p de $\mathbb{R}[X]$ de degré impair possède au moins une racine dans $\mathbb{R}$. En effet : $p : \mathbb{R} \to \mathbb{R}$ est continue et $\lim_{\pm\infty} p(x) = \pm\infty$), on en déduit :

$[K : \mathbb{R}]$ est pair

($[K : \mathbb{Q}] = 1$ étant impossible, car entrainant $K = \mathbb{R}$ en contradiction avec $K \supset \mathbb{C} \supsetneq \mathbb{R}$)

K est inclus dans le corps des racines de p sur $\mathbb{R}$. Si l'on montre que ce corps des racine n'est autre que $\mathbb{C}$, on aura $K = \mathbb{C}$. Dans la suite, on peut supposer que K est le corps des racines de p sur $\mathbb{R}$. (*)

p étant séparable (car tout polynôme irréductible sur un corps de caractéristique 0 est séparable, ex 3 p101 du queré) on aura (Pro. II) :

$$[K : \mathbb{R}] = \# G(K/\mathbb{R})$$

(*) sinon, introduisez une autre notation : " soit Σ le corps des racines de p sur $\mathbb{R}$ " et suivez la suite du raisonnement)

$G(K/\mathbb{R})$ admettra un 2-groupe de Sylow H d'ordre 2^m, et :

$$\# G(K/\mathbb{R}) = 2^m q \qquad q \text{ impair}$$

Soit $F = K^H$ le corps fixe de H. On sait que (Th. IV.1) :

$$\begin{cases} K \text{ est une extension galoisienne de } F \\ G(K/F) = H \\ [K:F] = \# H = 2^m \end{cases}$$

$$\mathbb{R} \subset F \subset K \Rightarrow \underbrace{[K:\mathbb{R}]}_{2^m q} = \underbrace{[K:F]}_{2^m} [F:\mathbb{R}] \Rightarrow [F:\mathbb{R}] = q$$

F étant une extension finie de $\mathbb{R}$ de caractéristique 0, il existera $\alpha \in F$ tel que $F = \mathbb{R}(\alpha)$ (Th. él. primitif, queré Co1 p103). Le polynôme irréductible $\mathrm{Irr}(\alpha, \mathbb{R}, X)$ de $\mathbb{R}[X]$ sera de degré $[F:\mathbb{R}] = q$ impair, donc $q=1$, $\underline{F = \mathbb{R} \text{ et } G(K/\mathbb{R}) = H}$.

$\mathbb{R} \subset \mathbb{C} \subset K$ donc $\mathbb{C}$ est un corps intermédiaire et son groupe de Galois $G_1 = G(K/\mathbb{C})$ sera un sous-groupe de $H = G(K/\mathbb{R})$. G_1 sera donc un 2-groupe.

* $\underline{\text{Si } G_1 \neq \{e\}}$, il contient un sous-groupe G_2 de cardinal $\# G_2 = \dfrac{\# G_1}{2}$ et $F' \doteq K^{G_2}$ vérifie (Th. IV.1) :

$$\begin{cases} \mathbb{C} \subset F' \subset K \\ G(K/F') = G_2 \\ [K:F'] = \# G_2 \end{cases}$$

$$\text{d'où } \underbrace{[K:\mathbb{C}]}_{=\# G_1} = \underbrace{[K:F']}_{\# G_2} \cdot [F':\mathbb{C}] \Rightarrow [F':\mathbb{C}] = \frac{\# G_1}{\# G_2} = 2$$

(car K = corps des racines de p séparable, et on utilise la Pro. II)

C'est absurde car $\mathbb{C}$ n'admet aucune extension de degré 2 (preuve : si $[F':\mathbb{C}]=2$, l'extension finie F' étant simple (queré Co1p103) on aurait $F'=\mathbb{C}(\beta)$. Le polynôme minimal $Irr(\beta,\mathbb{C},X)$ serait de degré 2 et irréductible sur $\mathbb{C}$, ce qui est absurde car tout polynôme de degré 2 sur $\mathbb{C}$ admet 2 racines.)

* Finalement $G_1=\{e\}=G(K/\mathbb{C})$ entraîne $K=\mathbb{C}$

Montrons le : $K\supsetneq\mathbb{C}$ entraine, $\mathbb{C}$ étant de caractéristique 0, que l'extension finie K de $\mathbb{C}$ est simple, soit $K=\mathbb{C}(\beta)$.
Soit $h=Irr(\beta,\mathbb{C},X)$ et $r=\deg h$.

$K\supsetneq\mathbb{C} \Rightarrow r\geq 3$ et l'on sait que $K=\mathbb{C}(\beta)=\{a_0+a_1\beta+\dots+a_{r-1}\beta^{r-1} / a_i\in\mathbb{C}\}$
On peut donc prolonger $Id_{\mathbb{C}}$ en un $\mathbb{C}$-automorphisme σ de K distinct de Id_K en posant $\sigma(\beta)=\beta^2$, d'où $G_1\neq\{e\}$.

CQFD

VII Application : Equations résolubles par radicaux

Dans ce §, K est un corps commutatif de caractéristique nulle. Sous cette hypothèse, rappelons que ([A] querré p104, Co1bis) :

L est une ext. galoisienne de K ssi c'est le corps des racines d'un polynôme de $K[X]$.

Théorème 1 : Si $a \in K^*$, le groupe de Galois du polynôme $X^n - a$ sur K est résoluble.

preuve :

1-cas : K contient une racine n-ième primitive de l'unité sur $\mathbb{Q}$, soit ε.

Si toutes les racines de $X^n - a$ sont dans K, $G(\Sigma/K) = G(K/K) = \{Id\}$ est résoluble. Supposons donc qu'il existe une racine α de $X^n - a$ telle que $\alpha \notin K$.

$\Omega = K(\alpha)$ sera le corps des racines de $X^n - a$ (car contenant toutes les racines $\varepsilon^i \alpha$, $0 \leq i \leq n-1$, de ce polynôme)

Tout K-automorphisme σ de $G(\Omega/K)$ sera parfaitement déterminé par l'image $\sigma(\alpha)$ qui est de la forme :

$$\sigma(\alpha) = \varepsilon^i \alpha$$

Soient $\sigma, \tau \in G(\Omega/K)$ avec $\sigma(\alpha) = \varepsilon^i \alpha$ et $\tau(\alpha) = \varepsilon^j \alpha$.

$$\text{De } \begin{cases} \sigma\tau(\alpha) = \sigma(\varepsilon^j \alpha) = \varepsilon^j . \varepsilon^i \alpha \\ \tau\sigma(\alpha) = \tau(\varepsilon^i \alpha) = \varepsilon^i \varepsilon^j \alpha \end{cases}$$

on déduit $\sigma\tau = \tau\sigma$ ie $G(\Omega/K)$ est commutatif, donc résoluble.

2e cas : K ne contient aucune racine n-ième primitive de l'unité.

Soit $\alpha \notin K$ une racine de $X^n - a$. On se ramène au 1er cas en introduisant $K' \doteq K(\varepsilon)$ où ε est une racine n-ième primitive de l'unité.

On a :

$$K \subset K' = K(\varepsilon) \subset \Omega = K(\varepsilon, \alpha)$$

Ω corps des racines de $X^n - a$ sur K' $\underset{(1^{er}\text{ cas})}{\Longrightarrow}$ $G(\Omega / K')$ résoluble

Ω corps des racines de $(X^n-1)(X^n-a)$ sur K $\Rightarrow$ Ω = ext. galoisienne de K

K' corps des racines de $X^n - 1$ sur K $\Rightarrow$ K' = ext. normale de K

On peut donc appliquer le Th IV.4 :

$$G(\Omega/K') \triangleleft G(\Omega/K)$$

$$\underbrace{G(\Omega/K) / G(\Omega/K')}_{\text{résoluble}} \simeq \underbrace{G(K'/K)}_{\text{résoluble}}$$

(car $\sigma, \tau \in G(K'/K)$ sont déterminés par l'image de ε. Soit $\sigma(\varepsilon) = \varepsilon^i$ et $\tau(\varepsilon) = \varepsilon^j$. On calcule :

$\sigma\tau(\varepsilon) = \varepsilon^{ij} = \tau\sigma(\varepsilon)$

donc $\sigma\tau = \tau\sigma$ et $G(K'/K)$ est commutatif)

$G(\Omega/K)$ sera bien résoluble comme quotient d'un groupe résoluble par un sous-groupe résoluble (Querré Th. 4 p 29)

CQFD

* Soit Σ un corps. Σ est <u>une extension de K par radicaux</u> s'il existe une suite d'extensions simples :

$$K = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_s = \Sigma$$

telles que $K_{i+1} = K_i(\alpha_i)$ et $\alpha_i^{n_i} = a_i \in K_i$

Une équation $f(x) = 0$ est dite <u>résoluble par radicaux</u> sur K si <u>toutes</u> ses racines appartiennent à une ext. de K par radicaux.

ex : $X^n - a$ est résoluble par radicaux sur K car si ε est une racine n-ième primitive de l'unité et si α est une racine de $X^n - a$, on a :

$$K \subset K(\varepsilon) \subset K(\varepsilon, \alpha) = \text{corps des racines de } X^n - a$$

avec $\varepsilon^n = 1 \in K$ et $\alpha^n = a \in K(\varepsilon)$ (en fait $a \in K$)

On peut alors généraliser le Th. 1 :

Théorème 2 :

Si Σ est une extension normale de K par radicaux, alors $G(\Sigma/K)$ est résoluble.

preuve :

Soient $\Omega_0 = K$ et Ω_{i+1} le corps des racines de $X^{n_i} - a_i$ sur Ω_i.

$$\begin{array}{ccccccc} K = \Omega_0 & \subset & \Omega_1 & \subset & \dots & \subset & \Omega_s \\ \cup & & \cup & & & & \cup \\ K = K_0 & \subset & K_1 & \subset & \dots & \subset & K_s = \Sigma = \text{ext. normale de } K \text{ par radicaux} \end{array}$$

où $K_{i+1} = K_i(\alpha_i)$ et $\alpha_i^{n_i} = a_i \in K_i$

1) <u>Montrons que : $G(\Omega_s/K)$ résoluble $\Rightarrow$ $G(\Sigma/K)$ résoluble</u>

Ω_s est une ext. galoisienne de K (car c'est une ext. finie et normale de K)

$K \subset \Sigma \subset \Omega_s$ et Σ est une ext. normale de K. Le Th IV.4 entraîne :

$$G(\Sigma/K) \simeq \frac{G(\Omega_s/K)}{G(\Omega_s/\Sigma)}$$

et $G(\Sigma/K)$ sera résoluble comme quotient d'un groupe résoluble (Queré ex 2 p 29)

2) Montrons que $G(\Omega_s/K)$ est résoluble :

* Ω_s est une extension galoisienne de K, donc sera une extension galoisienne de Ω_{s-2} (car finie et normale sur Ω_{s-2}, d'après la Pro. III.1)

Ω_{s-1} est une extension normale de Ω_{s-2} (comme corps des racines du polynôme $X^{n_{s-2}} - a_{s-2}$ sur Ω_{s-2}) et :

$$\Omega_{s-2} \subset \Omega_{s-1} \subset \Omega_s$$

Le Th. IV.4 entraîne :

$$G(\Omega_s/\Omega_{s-2})\Big/G(\Omega_s/\Omega_{s-1}) \simeq G(\Omega_{s-1}/\Omega_{s-2})$$

$G(\Omega_s/\Omega_{s-1})$ résoluble (Th.1) ; $G(\Omega_{s-1}/\Omega_{s-2})$ résoluble (Th.1)

et $G(\Omega_s/\Omega_{s-2})$ sera résoluble.

* Au pas suivant :

$$\Omega_{s-3} \subset \Omega_{s-2} \subset \Omega_s$$

Ω_s = ext. galoisienne de Ω_{s-3} (car finie et normale sur Ω_{s-3}, Pro III.1)

Ω_{s-2} = ext. normale de Ω_{s-3} (comme corps des racines de $X^{n_{s-3}} - a_{s-3}$)

Le Th. IV 4 entraîne encore :

$$G(\Omega_s/\Omega_{s-3})\Big/G(\Omega_s/\Omega_{s-2}) \simeq G(\Omega_{s-2}/\Omega_{s-3})$$

$G(\Omega_s/\Omega_{s-2})$ résoluble (hyp. récurrente) ; $G(\Omega_{s-2}/\Omega_{s-3})$ résoluble (Th.1)

On achève la démonstration par une récurrence finie.

CQFD

Théorème 3 :

Toute extension de K par radicaux est contenue dans une extension normale de K par radicaux.

preuve : On a

$$K = K_0 \subset K_1 \subset \dots \subset K_s = \Sigma \qquad K_{i+1} = K_i(\alpha_i) \quad \text{et} \quad \alpha_i^{n_i} = a_i \in K_i$$

Montrons par récurrence sur $i \in [0, s]$ que :

Il existe un corps Δ_i contenant Σ et un corps Ω_i, Ω_i étant une ext. galoisienne de K par radicaux, contenant K_i :

Δ_i ; Σ ; Ω_i = ext. gal. de K par radicaux ; K_i ; K

ce qui entrainera le Th. 3 (Ω_s vérifiant alors $\Omega_s \supset K_s = \Sigma$)

C'est vrai si $i = 0$ (prendre $\Omega_0 = K$ et $\Delta_0 = \Sigma$).

Montrons la propriété au rang $i+1$:

Posons : $G_i = G(\Omega_i / K)$

$\{\gamma_1, \dots, \gamma_{s_i}\}$ = él. distincts de l'ensemble $\{\sigma(a_i) / \sigma \in G_i\}$

$$g_i(X) = \prod_{j=1}^{s_i} (X^{n_i} - \gamma_j) \qquad \in \Omega_i[X]$$

* Tout automorphisme σ de G_i permute les éléments $\gamma_1, \dots, \gamma_{s_i}$, donc $\sigma g_i = g_i$ et les coefficients de $g_i(X)$ seront dans le corps fixe $\Omega_i^{G(\Omega_i/K)} = K$ (car Ω_i est une ext. gal. de K, Th IV. 2).

Donc $g_i \in K[X]$.

Théorème
Si une

* Soit Δ_{i+1} le corps des racines de g_i sur Δ_i. On a :

$$\Delta_{i+1} = \Delta_i(\alpha_i, \alpha_i', \dots, \alpha_i^{(h)})$$

où $\alpha_i, \dots, \alpha_i^{(h)}$ sont les racines de g_i n'appartenant pas à Δ_i

Soit $\Omega_{i+1} = \Omega_i(\alpha_i, \alpha_i', \dots, \alpha_i^{(h)})$

1) Ω_{i+1} contient Ω_i, donc K_i, et α_i, donc contiendra $K_{i+1} = K_i(\alpha_i)$

2) Ω_i étant une ext. normale de K, c'est le corps des racines d'un polynôme $f_i \in K[X]$. Ω_{i+1} sera donc le corps des racines du polynôme $f_i g_i \in K[X]$, et par suite une ext. galoisienne de K

3) Ω_{i+1} sera une ext. par radicaux de K car si $0 \leq k \leq h$,

$$g_i(\alpha_i^{(k)}) = 0 \Rightarrow (\alpha_i^{(k)})^{n_i} = \gamma_j \quad \text{pour } j \in [1, s_i]$$

ce qui montre que Ω_{i+1} s'obtient, à partir de Ω_i, par adjonctions finies de radicaux.

CQFD

Théorème 4

Si une équation est résoluble par radicaux, alors son groupe de Galois est résoluble.

(La Réc. serait vraie (?) cf Une histoire des math. Coll. Points)

preuve :

Soit $f(X)=0$ une équation résoluble par radicaux. Il existe une extension F de K par radicaux contenant toutes les racines de f, donc contenant le corps des racines Σ de f sur K.

Le Th. 3 assure l'existence d'une ext. Ω de K par radicaux qui contienne F et qui soit normale sur K.

Gr ama :

$$K \subset \Sigma \subset \Omega$$

Σ normal sur K (comme corps des racines de f sur K)

Ω est une ext. gal. de K (car ext. normale par radicaux de K, donc normale et finie de K)

Le Th. IV.4 implique :

$$\begin{cases} G(\Omega/\Sigma) \lhd G(\Omega/K) \\ G(\Omega/K)/G(\Omega/\Sigma) \simeq G(\Sigma/K) \end{cases}$$

résoluble (Th. 2)

$G(\Sigma/K)$ sera résoluble comme quotient d'un groupe résoluble.

(quotient)

CQFD

Il faut montrer

Théorème 5 :

Soit $n \geq 5$ donné. Il existe un corps L contenant K et un polynôme irréductible f sur L de degré n tels que $f(X)=0$ ne soit pas résoluble par radicaux sur L.

preuve :

Soient $F = K(Y_1, Y_2, \dots, Y_n)$ = corps des fractions rationnelles en $Y_1, \dots, Y_n$ sur K

$$f(X) = \prod_{i=1}^{n} (X - Y_i) = X^n + \sum_{k=1}^{n} (-1)^k s_k X^{n-k}$$

où s_k = fct sym. élém. de degré k des $Y_1, \dots, Y_n$

$$L = K(s_1, \dots, s_n)$$

Alors :

* F sera le corps des racines de $f \in L[X]$, ie $F = L(Y_1, \dots, Y_n)$

* Le groupe de Galois $G(F/L)$ de $f \in L[X]$ est $\mathcal{S}_n$:

En effet, $\mathcal{S}_n$ opère sur le corps $F = K(Y_1, \dots, Y_n)$ par :

$$\begin{aligned} \mathcal{S}_n \times F &\longrightarrow F \\ \sigma, g &\longmapsto \sigma g \quad \text{tq} \quad \sigma g(Y_1, \dots, Y_n) = g(Y_{\sigma(1)}, \dots, Y_{\sigma(n)}) \end{aligned}$$

qui nous permet de définir le monomorphisme de groupes :

$$\begin{aligned} \mathcal{S}_n &\longrightarrow \mathrm{Aut}\, F \\ \sigma &\longmapsto \{ g \mapsto \sigma g \} \end{aligned}$$

Soit S_n l'image de $\mathcal{S}_n$ par ce morphisme. S_n est un sgroupe de $\mathrm{Aut}\, F$ et le Th. IV.1 permet de constater que :

- F est une ext. galoisienne du corps fixe $k = F^{S_n}$
- $G(F/F^{S_n}) = S_n \simeq \mathcal{S}_n$
- $[F : F^{S_n}] = \# \mathcal{S}_n = n!$

Il faut montrer que $L = F^{S_n}$ pour conclure :

$g \in F^{S_n} \iff \forall \sigma \in \mathcal{S}_n \quad \sigma g = g \iff g$ est une fraction rationnelle symétrique.

L'expression $f(X) = \prod_{i=1}^{n} (X - Y_i)$ montre que $\sigma f = f$ dès que $\sigma \in \mathcal{S}_n$

et permet d'affirmer que les coefficients s_k de ce polynôme seront tous dans F^{S_n} (on les appelle les fractions rationnelles symétriques "élémentaires")

Ainsi :

$$L = K(s_1, \dots, s_n) \subset F^{S_n} \Rightarrow [F : L] \geq [F : F^{S_n}] = n! \qquad (1)$$

F est le corps des racines de $f \in L[X]$, séparable, donc (Pro. II) :

$$\# G(F/L) = [F : L] \quad \text{divise } n! \qquad (2)$$

(1) et (2) entraînent $[F:L] = [F : F^{S_n}]$ d'où $L = F^{S_n}$.

Ccl : $G(F/L) \simeq \mathcal{S}_n$ n'est pas résoluble pour $n \geq 5$ (queré Co1 p34)

donc (Th. 4) $f(X) = 0$ ne sera pas résoluble par radicaux.

CQFD

IV Théorèmes fondamentaux de la Théorie de Galois

Th 1 K corps
G sgroupe de $Aut(K)$
K^G = corps fixe de $K \doteq \{x \in K \,/\, \forall \sigma \in G \;\; \sigma(x) = x\}$

Alors K = ext. gal. de K^G
$G(K/K^G) = G$
$[K : K^G] = \#G$

$k = K^G$ $\quad n = \#G$

a) K = ext. séparable de k

$\alpha \in K$ $\quad A = \{\sigma_1, \dots, \sigma_r\}$ = ens. maximal d'él. de G tq $\sigma_1(\alpha), \dots, \sigma_r(\alpha)$ distincts 2à2.

$\exists j \quad \sigma_j(\alpha) = \alpha \qquad (\text{car } Id_k(\alpha) = \alpha)$

α est racine de $f(X) = \prod_{i=1}^{r} (X - \sigma_i(\alpha))$

$\sigma f(X) = f(X) \Rightarrow f \in k[X]$

Ccl : f est séparable et s'annule en α

b) K = ext. normale

Si p est un polynôme irréductible de $k[X]$ ayant une racine α dans k, alors $p \mid f \Rightarrow$ toutes les racines de p sont dans K.

c) K = ext. finie

$\forall \alpha \in K \quad p = \mathrm{Irr}(\alpha, k, X) \mid f(X)$ donc $\deg p \leq n$

Soit $\alpha \in K$ de degré maximum $m \leq n$

$k(\alpha) \neq K \Rightarrow \exists \beta \in K \setminus k(\alpha)$ et $k(\alpha, \beta) = k(\gamma)$ (Th. él. primitif)

donc $[k(\alpha,\beta) : k] = \underbrace{[k(\alpha,\beta) : k(\alpha)]}_{>1} \cdot \underbrace{[k(\alpha) : k]}_{m} > m$ absurde

Ccl : $[K : k] = m \leq n$

d)

K ext. gal. de $k \Rightarrow K$ = corps des racines d'un poly. séparable g

$\Rightarrow \#G(K/k) = [K : k] \leq n$

Mais $G \subset G(K/k) \Rightarrow n \leq \#G(K/k)$

D'où $G = G(K/k)$ et $\#G = [K : k]$

CQFD

Th 2 K = ext. gal. de k

1) $k = K^{G(K/k)}$

2) $k \subset F \subset K \Rightarrow K$ = ext. gal. de F
(corps int.)

3) $\mathcal{K}$ = famille des corps int.
$\mathcal{G}$ = " des sgroupes de $G(K/k)$

$\mathcal{K} \longrightarrow \mathcal{G}$ est une bijection décroissante.
$F \longmapsto G(K/F)$

$G \doteq G(K/k)$

1) $k \subset K^G$ est trivial

Réc., soit $\alpha \in K^G$.

$p = \mathrm{Irr}(\alpha, k, X)$ séparable $\Rightarrow$ $\mathrm{Id}_k : k \to k$ se prolonge de $\deg p$ façons en un monomorphisme $\sigma : k(\alpha) \longrightarrow \bar{K}$

σ se prolonge en σ^* (Th III.1) :

$$\begin{array}{ccc} k(\alpha) & \xrightarrow{\sigma} & \bar{K} = \bar{k} \text{ alg. clos} \\ \downarrow & \nearrow_{\sigma^*} & \\ K & & \\ \text{ext. alg. de } k & & \end{array}$$

K ext. normale de $k \Rightarrow \sigma^* = k$-automorphisme de K (Th III.2)

$\Rightarrow \sigma^*(\alpha) = \sigma(\alpha) = \alpha$ (car $\alpha \in K^G$)

Cl : $\exists !$ prolongement de Id_k en $\sigma : k(\alpha) \longrightarrow \bar{K}$.

Donc $\deg p = 1 \Rightarrow \alpha \in k$.

2) Conséquence des Pro III.1 et III.2

3) $\begin{array}{ccc} \mathcal{K} & \xrightarrow{\Psi} & \mathcal{G} \\ F & \longmapsto & G(K/F) \end{array}$

$\forall H \in \mathcal{G}$ $k \subset K^H \subset K$ et $G(K/K^H) = H$ (Th 1)

d'où la surjectivité.

$G(K/F) = G(K/F') \overset{1)}{\Rightarrow} F = K^{G(K/F)} = K^{G(K/F')} = F'$ d'où l'injectivité.

Décroissance triviale.

Th 3 K = ext. gal. de k

F et F' corps intermédiaires k-isomorphes $\Rightarrow$ $G(K/F)$ et $G(K/F')$ sont conjugués dans $G(K/k)$

$\exists \lambda$ k-aut. tq

$$\begin{array}{ccc} F & \xrightarrow{\sim} & F' \\ \downarrow & & \downarrow \\ K & \xrightarrow{\lambda} & K \end{array}$$

(car K ext. normale de k $\Rightarrow$ K = corps des racines d'un polynôme p de $k[X]$, donc à fortiori d'un poly. p de $F[X]$ (ou $F'[X]$) et on applique Th I)

$\sigma \in G(K/F) \Rightarrow \lambda \sigma \lambda^{-1} \in G(K/F')$

$\sigma' \in G(K/F') \Rightarrow \lambda^{-1} \sigma \lambda \in G(K/F)$

Finalement $G(K/F') = \lambda\, G(K/F)\, \lambda^{-1}$.

Th 4 : K ext. gal. de k
F corps intermédiaire

1) F normal sur k $\iff$ $G(K/F) \triangleleft G(K/k)$

2) Si F est normal sur k, alors $G(K/k)/G(K/F) \simeq G(F/k)$

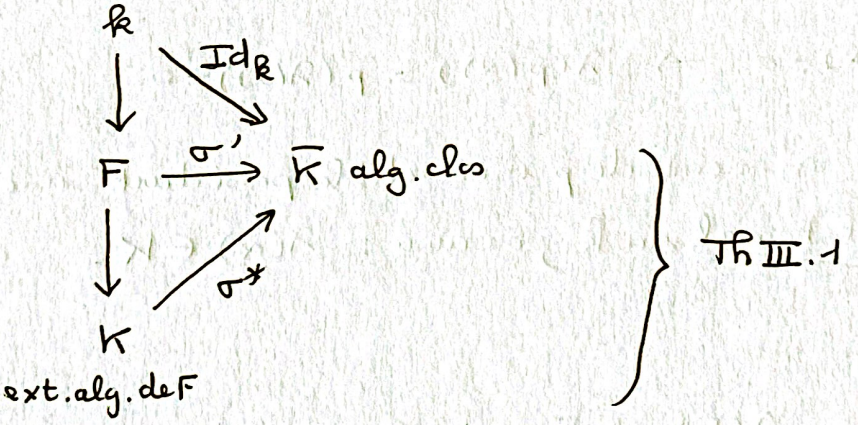
* Si F est normal sur k, on peut définir :

$$h : G(K/k) \longrightarrow G(F/k), \quad \sigma \longmapsto \sigma|_F$$

(car F normal sur k $\Rightarrow$ le prolongement $\sigma|_F : F \to \bar{k}$ de $Id_k : k \to \bar{k}$ sera un F-automorphisme (Th III.2))

* h surjective :

$\forall \sigma' \in G(F/k)$ $\exists \sigma^*$ prolongeant σ' tq



K normal sur k $\underset{\text{Th III.2}}{\Longrightarrow}$ $\sigma^* =$ k-automorphisme de K

Clairement : $\sigma^*|_F = \sigma'$

* $\sigma \in \ker h \iff \sigma|_F = Id_F \iff \sigma \in G(K/F)$

Donc $= G(K/F)$ et $\dfrac{G(K/k)}{G(K/F)} \simeq G(F/k)$

* Si F n'est pas normal sur k, il existe un monomorphisme λ tq :

$$\begin{array}{ccc} k & \xrightarrow{Id_k} & \bar{k} = \bar{K} \\ \downarrow & \nearrow_{\lambda} & \\ F & & \end{array}$$

et $\lambda \neq k$-automorphisme de F (Th III.2)

$\lambda(F) \neq F$ sinon $\lambda : F \to F$ serait un endomorphisme injectif du k-espace vectoriel de dim. finie F, donc un k-aut.

$k \subset \lambda(F) \subset K$

car $\forall \alpha \in F \quad p = Irr(\alpha, k, X)$

$p(\alpha) = 0 \Rightarrow \lambda(p(\alpha)) = p(\lambda(\alpha)) = 0$

$\lambda(\alpha)$ sera racine de p irréductible possédant une racine α dans F. K étant normal sur k, on aura : $\lambda(\alpha) \in K$.

Ccl : $\lambda(F)$ et F sont 2 corps intermédiaires k-isomorphes et distincts. Le Th 3 entraîne :

$G(K/\lambda(F))$ et $G(K/F)$ sont conjugués

Ces 2 sgroupes étant distincts (Th 2) on aura bien :

$G(K/F)$ n'est pas distingué.

V Application : Recherche des sous-corps d'une ext. gal. de $\mathbb{Q}$

Exposer l'exemple b) p 20-21 seulement